 (12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003 年6 月12 日 (12.06.2003)

PCT

(10) 国際公開番号
WO 03/049362 A1

(51) 国際特許分類[7]: H04L 9/08, G06F 17/60, 15/00

(21) 国際出願番号: PCT/JP02/12356

(22) 国際出願日: 2002 年11 月27 日 (27.11.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-373674 2001 年12 月7 日 (07.12.2001) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 石井 秀浩 (ISHII,Hidehiro) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 稲本 義雄 (INAMOTO,Yoshio); 〒160-0023 東京都 新宿区 西新宿７丁目１１番１８号 ７１１ビルディング４階 Tokyo (JP).

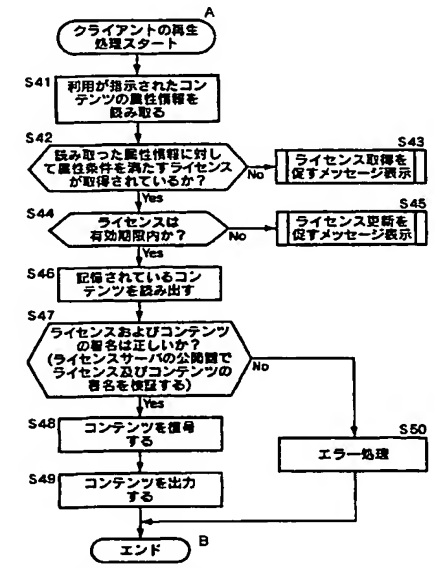
(81) 指定国 (国内): CA, CN, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

[続葉有]

(54) Title: INFORMATION PROCESSING APPARATUS AND METHOD

(54) 発明の名称: 情報処理装置および方法




A...CLIENT REPRODUCTION START
S41...READ ATTRIBUTE INFORMATION OF CONTENT SPECIFIED TO BE USED
S42...LICENSE ACQUIRED SATISFIES ATTRIBUTE CONDITION FOR THE ATTRIBUTE INFORMATION READ
S43...DISPLAY MESSAGE PROMPTING TO ACQUIRE LICENSE
S44...LICENSE WITHIN A VALID TERM?
S45...DISPLAY MESSAGE PROMPTING TO UPDATE LICENSE
S46...READ OUT CONTENT STORED
S47...LICENSE AND CONTENT SIGNATURE AUTHENTIC? (AUTHENTICATE THE LICENSE AND CONTENT SIGNATURE BY USING PUBLIC KEY OF LICENSE SERVER)
S48...DECRYPT CONTENT
S50...ERROR PROCESSING
S49...OUTPUT CONTENT
B...END

(57) Abstract: When a client reproduces a content, attribute information is read from the header of the content data corresponding to the content ID specified by the user. When the attribute information which has been read satisfies the attribute condition described in the license stored in the storage unit, encrypted content data is decrypted and output. After delivering a content, for example, by issuing a license having an attribute condition specifying a release date and artist, it is possible to sell a best version and a collection without creating a new content. If a license having a particular subscription ID as the attribute condition is defined, a user having the license can use a newly released content having the subscription ID without purchasing an additional license.

[続葉有]

WO 03/049362 A1

添付公開書類:
— 国際調査報告書



(57) 要約:

クライアントがコンテンツを再生する場合、ユーザが指示したコンテンツＩＤに対応するコンテンツデータのヘッダに記述されている属性情報を読み取る。読みとった属性情報が、記憶部に記憶されているライセンスに記述されている属性条件を満たすものである場合、暗号化されているコンテンツデータを復号して出力する。

コンテンツを配布後、例えばリリース日とアーティストを制約した属性条件を持つライセンスを発行することで、コンテンツを新たに作成することなく、ベスト版や全集を新たに発売することができる。属性条件として特定のサブスクリプションＩＤを持つライセンスを定義すれば、そのライセンスを持っているクライアントは、そのサブスクリプションＩＤを持つ新譜のコンテンツを、ライセンスを追加購入することなく使用することができる。

# 明細書

## 情報処理装置および方法

### 技術分野

本発明は、情報処理装置および方法に関し、特に、著作権者からライセンスを受けていないコンテンツが不正にコピーされ、利用されるのを防止することができるようにした、情報処理装置および方法に関する。

### 背景技術

最近、インターネットを介して、ユーザが、自分自身が保持している音楽データを他のユーザに提供し、自分自身が保持していない音楽データを他のユーザから提供を受けるようにして、複数のユーザが無料で音楽データを交換しあうシステムが実現されている。

このようなシステムでは、理論的には、１つの音楽、その他のコンテンツが存在すれば、他の全てのユーザが、それを利用することが可能となり、多くのユーザがコンテンツを購入しなくなるため、コンテンツに関する著作権者は、著作物としてのコンテンツが売れないため、著作物の販売に伴い、本来受け取ることが可能な著作物の利用に関するロイヤリティを受け取る機会を失うことになる。

そこで、配布されるコンテンツは暗号化しておき、そのコンテンツを利用するためのライセンスを別途発行し、暗号化されたコンテンツに対応するライセンスを持っていないとコンテンツを復号、再生できないようにするようにしたシステムがある。

このようにすることでコンテンツを自由に配布することを可能としつつ、著作物の著作権を保護することができる。

しかしながら、上記のシステムでは、ライセンスとコンテンツの対応関係を柔軟に設定したり、既に配布されたライセンスよって利用できるコンテンツを新たに配布することが難しかった。

発明の開示

本発明はこのような状況に鑑みてなされたものであり、コンテンツは自由に配布・流通させ、ライセンスによって利用できるコンテンツの集合を自由に設定することができるようにするものである。

本発明の第１の情報処理装置は、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信手段と、前記コンテンツを記憶するコンテンツ記憶手段と、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信手段と、前記ライセンスを記憶するライセンス記憶手段と、前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを判定する判定手段と、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号手段と、前記復号手段により復号されたコンテンツデータを出力する出力手段とを備えることを特徴とする。

前記コンテンツは、更に前記コンテンツデータを復号するためのコンテンツキーを含むようにすることができる。

前記属性情報は、属性項目と属性値の組み合わせから構成することができる。

前記属性項目はレコード会社、アーティスト、リリース日、コンテンツ発行者、ジャンル、サブスクリプション、またはレーベルに関する情報を含むようにすることができる。

前記属性条件は属性項目、属性値、及び演算子の組み合わせから構成することができる。

本発明の第２の情報処理装置は、コンテンツに含まれる属性情報に関する条件を記載した属性条件を含むライセンスを一意に識別するライセンス ID を含むライセンス要求を受信する受信手段と、ライセンスをライセンス ID と共に記憶する記憶手段と、前記ライセンス要求に含まれる前記ライセンス ID に対応する前

記ライセンスを取り込む取り込み手段と、前記ライセンスに電子署名を付加する署名手段と、署名手段により署名されたライセンスを送信する送信手段とを備えることを特徴とする。

更に、前記取り込み手段によって取り込まれたライセンスに端末 ID を付加するライセンス処理手段を備えることができる。

本発明の第３の情報処理装置は、暗号化コンテンツデータと属性情報とを含むコンテンツを記憶する記憶手段と、コンテンツを一意に識別するコンテンツ ID を含むコンテンツ要求を受信する受信手段と、コンテンツ要求に含まれるコンテンツ ID に対応するコンテンツを送信する送信手段とを備える情報処理装置であって、前記コンテンツに含まれる前記属性情報は、当該コンテンツを利用する際にライセンスの属性条件を満たすか否かを判断するために用いられる情報であり、前記ライセンスの属性条件は利用できる前記コンテンツの前記属性情報に関する条件を記載した情報であることを特徴とする。

本発明の情報処理方法は、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとを含むことを特徴とする。

本発明のプログラムは、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセン

スを記憶するライセンス記憶ステップと、前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムである。

本発明のプログラム格納媒体に格納されているプログラムは、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムである。

## 図面の簡単な説明

図１は、本発明を適用したコンテンツ提供システムの構成を示すブロック図である。

図２は、図１のクライアントの構成を示すブロック図である。

図３は、図１のクライアントのコンテンツのダウンロード処理を説明するフローチャートである。

図４は、図１のコンテンツサーバのコンテンツ提供処理を説明するフローチャートである。

図５は、データフォーマットの例を示す図である。

図６は、属性項目の種類を説明する図である。

図７は、ライセンスの構成を示す図である。

図８は、クライアントの再生処理を説明するフローチャートである。

図９は、ライセンス取得処理を説明するフローチャートである。

図１０は、ライセンス取得処理を説明するフローチャートである。

図１１は、ライセンス取得処理を説明するフローチャートである。

図１２は、ライセンス取得処理の詳細を説明するフローチャートである。

図１３は、コンテンツデータを取得する処理を説明するフローチャートである。

図１４は、キーの構成を説明する図である。

図１５は、キーの構成とライセンスの関係を説明する図である。

図１６は、ライセンスサーバのライセンス付与処理を説明する図である。

発明を実施するための最良の形態

図１は、本発明を適用したコンテンツ提供システムの構成を示している。インターネット２には、クライアント１－１，１－２（以下、これらのクライアントを個々に区別する必要がない場合、単にクライアント１と称する）が接続されている。この例においては、クライアントが２台のみ示されているが、インターネット２には、任意の台数のクライアントが接続される。

また、インターネット２には、クライアント１に対してコンテンツを提供するコンテンツサーバ３、コンテンツサーバ３が提供するコンテンツを利用するのに必要なライセンスをクライアント１に対して付与するライセンスサーバ４、およびクライアント１がライセンスを受け取った場合に、そのクライアント１に対して課金処理を行う課金サーバ５が接続されている。

これらのコンテンツサーバ３、ライセンスサーバ４、および課金サーバ５も、任意の台数、インターネット２に接続される。

図２はクライアント１の構成を表している。

図２において、CPU（Central Processing Unit）２１は、ROM（Read Only Memory）２２に記憶されているプログラム、または記憶部２８からRAM（Random Access Memory）２３にロードされたプログラムに従って各種の処理を実行する。タイマ２０は、計時動作を行い、時刻情報をCPU２１に供給する。RAM２３にはまた、CPU２１が各種の処理を実行する上において必要なデータなども適宜記憶される。

暗号化復号部２４は、コンテンツデータを暗号化するとともに、既に暗号化されているコンテンツデータを復号する処理を行う。コーデック部２５は、例えば、ATRAC（Adaptive Transform Acoustic Coding）３方式などでコンテンツデータをエンコードし、入出力インタフェース３２を介してドライブ３０に接続されている半導体メモリ４４に供給し、記録させる。あるいはまた、コーデック部２５は、ドライブ３０を介して半導体メモリ４４より読み出した、エンコードされているデータをデコードする。

半導体メモリ４４は、例えば、メモリスティック（商標）などにより構成される。

CPU２１、ROM２２、RAM２３、暗号化復号部２４、およびコーデック部２５は、バス３１を介して相互に接続されている。このバス３１にはまた、入出力インタフェース３２も接続されている。

入出力インタフェース３２には、キーボード、マウスなどよりなる入力部２６、CRT、LCDなどよりなるディスプレイ、並びにスピーカなどよりなる出力部２７、ハードディスクなどより構成される記憶部２８、モデム、ターミナルアダプタなどより構成される通信部２９が接続されている。通信部２９は、インターネット２を介しての通信処理を行う。通信部２９はまた、他のクライアントとの間で、アナログ信号またはデジタル信号の通信処理を行う。

入出力インタフェース３２にはまた、必要に応じてドライブ３０が接続され、磁気ディスク４１、光ディスク４２、光磁気ディスク４３、或いは半導体メモリ

４４などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部２８にインストールされる。

なお、図示は省略するが、コンテンツサーバ３、ライセンスサーバ４、課金サーバ５も、図２に示したクライアント１と基本的に同様の構成を有するコンピュータにより構成される。

次に、図３のフローチャートを参照して、クライアント１がコンテンツサーバ３からコンテンツの提供を受ける処理について説明する。

ユーザが、入力部２６を操作することでコンテンツサーバ３に対するアクセスを指令すると、CPU２１は、通信部２９を制御し、インターネット２を介してコンテンツサーバ３にアクセスさせる。ステップＳ２において、ユーザが、入力部２６を操作して、提供を受けるコンテンツを指定すると、CPU２１は、この指定情報を受け取り、通信部２９から、インターネット２を介してコンテンツサーバ３に、指定されたコンテンツのコンテンツＩＤを通知する。図４のフローチャートを参照して後述するように、この通知を受けたコンテンツサーバ３は、通知されたコンテンツＩＤに対応する、暗号化されたコンテンツデータを含むコンテンツを送信してくるので、ステップＳ３において、CPU２１は、通信部２９を介して、このコンテンツを受信すると、ステップＳ４において、コンテンツを記憶部２８を構成するハードディスクに供給し、記憶させる。

次に、図４のフローチャートを参照して、クライアント１の以上の処理に対応するコンテンツサーバ３のコンテンツ提供処理について説明する。なお、以下の説明において、図２のクライアント１の構成は、コンテンツサーバ３の構成としても引用する。

ステップＳ２１において、コンテンツサーバ３のCPU２１は、インターネット２から通信部２９を介してクライアント１よりアクセスを受けるまで待機し、アクセスを受けたと判定したとき、ステップＳ２２に進み、クライアント１から送信されてきたコンテンツを指定するコンテンツＩＤを取り込む。このコンテンツ

を指定する情報は、クライアント１が、図３のステップＳ２において通知してきたコンテンツＩＤである。

ステップＳ２３において、コンテンツサーバ３のCPU２１は、記憶部２８に記憶されているコンテンツデータの中から、ステップＳ２２の処理で取り込まれた情報で指定されたコンテンツを読み出す。CPU２１は、ステップＳ２４において、記憶部２８から読み出されたコンテンツデータを、暗号化復号部２４に供給し、暗号化させる。

記憶部２８に記憶されているコンテンツデータは、コーデック部２５により、既にATRAC３方式によりエンコードされているので、このエンコードされているコンテンツデータが暗号化されることになる。

なお、もちろん、記憶部２８に予め暗号化した状態でコンテンツデータを記憶させることができる。この場合には、ステップＳ２４の処理は省略することが可能である。

次に、ステップＳ２５において、コンテンツサーバ３のCPU２１は、暗号化したコンテンツデータを伝送するフォーマットを構成するヘッダに、暗号化されているコンテンツデータを復号するのに必要なキーと、コンテンツに関する各種情報を示す属性情報を付加する。そして、ステップＳ２６において、コンテンツサーバ３のCPU２１は、ステップＳ２４の処理で暗号化されたコンテンツデータと、ステップＳ２５の処理でキーと属性情報及びその電子署名を付加したヘッダとをフォーマット化したコンテンツを、通信部２９から、インターネット２を介して、アクセスしてきたクライアント１に送信する。

図５は、このようにして、コンテンツサーバ３からクライアント１にコンテンツが供給される場合のフォーマットの構成を表している。同図に示されるように、このフォーマットは、ヘッダ（Header）とデータ（Data）とにより構成される。

ヘッダには、属性情報（Attribute List）及び属性情報をライセンスサーバの暗号鍵で署名した電子署名、イネーブリングキーブロック（EKB（Enabling Key Block））および、EKBをDNKを用いて復号処理することによって得られる

ルートキーKRにより暗号化されたコンテンツキーKc（KR（Kc））が配置されている。

属性情報には属性項目と属性値との組み合わせからなる属性のエントリーが複数記述されている。

属性項目の種類を図６に示す。CID、RCID、CIID、AID、GID及びLIDはそれぞれコンテンツ、レコード会社、コンテンツ発行者、アーティスト、ジャンル及びレーベルを一意に識別するIDである。RelDateはコンテンツのリリース日を表す。サブスクリプションIDは後述するサブスクリプションライセンスに用いられる属性項目である。

URLは、コンテンツを利用するためのライセンスを取得するときアクセスするアドレス情報であり、図１のシステムの場合、具体的には、ライセンスを受けるために必要なライセンスサーバ４のアドレスである。

データは、任意の数の暗号化ブロック（Encryption block）により構成される。各暗号化ブロックは、イニシャルベクトル（IV（Initial Vector））、シード（Seed）、およびコンテンツデータをキーK'cで暗号化したデータEK'c(data)により構成されている。

キーK'cは、次式により示されるように、コンテンツキーKcと、乱数で設定される値Seedをハッシュ関数に適応して演算された値により構成される。

K'c＝Hash(Kc, Seed)

イニシャルベクトルIVとシードSeedは、各暗号化ブロック毎に異なる値に設定される。

この暗号化は、コンテンツのデータを８バイト単位で区分して、８バイト毎に行われる。後段の８バイトの暗号化は、前段の８バイトの暗号化の結果を利用して行われるCBC（Cypher Block Chaning）モードで行われる。

CBCモードの場合、最初の８バイトのコンテンツデータを暗号化するとき、その前段の８バイトの暗号化結果が存在しないため、最初の８バイトのコンテンツ

データを暗号化するときは、イニシャルベクトルIVを初期値として暗号化が行われる。

このCBCモードによる暗号化を行うことで、１つの暗号化ブロックが解読されたとしても、その影響が、他の暗号化ブロックにおよぶことが抑制される。

なお、この暗号化については、図１４と図１５を参照にして、後に詳述する。

以上のようにして、クライアント１は、コンテンツサーバ３からコンテンツを無料で、自由に取得することができる。

しかしながら、各クライアント１は、取得したコンテンツを利用するとき、ライセンスを取得する必要がある。

ライセンスを取得する際には、クライアント１は事前にライセンスサーバにオンラインあるいはオフラインで登録処理を行い、サービスデータを取得しておく。サービスデータにはデバイスノードキー（DNK）及び端末IDが含まれており、EKBを復号処理するのに用いられる。サービスデータ及びライセンスサーバから取得するライセンスはクライアント１の記憶部２８にセキュアに保存される。

図７にライセンスの構成を示す。ライセンスにはライセンスID、タイムスタンプ、使用期限、属性条件、使用規則、及びこれらをライセンスサーバの秘密鍵で署名した電子署名が含まれる。タイムスタンプはライセンスの発行日を表す。使用期限はライセンスを使用できる期限日を表し、この期限日を過ぎるとそのライセンスは使用できなくなる。属性条件はそのライセンスを所持しているクライアント１が利用できるコンテンツの属性の条件を属性項目と属性項目に関する値、比較演算子、及び論理演算子の組み合わせからなる条件式によって表したものである。使用規則にはそのライセンスの利用できるコンテンツを使用するための規則を記述したものであり、サービスデータに含まれているものと同じ端末IDが含まれる。

以下に、コンテンツに含まれる属性情報、及びライセンスに含まれる属性条件との組み合わせによって実現可能なライセンス構成の例を示す。

コンテンツc1の属性情報には、次のように記述されている。

c1: cid = {1}, aid = {0, 1}, reldate = 2000年11月10日

これは、コンテンツIDは1、アーティストIDは0および1（即ち、0番のアーティストと1番のアーティストの合作）、リリース日は2000年11月10日であるということを表す。

同様に、コンテンツc2, c3, c4の属性情報に、次のように記述されている。

c2: cid = {2}, aid = {0}, reldate = 2000年12月20日

c3: cid = {3}, aid = {0}, reldate = 2001年3月1日

c4: cid = {4}, aid = {0}, reldate = 2001年10月21日

一方、ライセンス11の属性条件には、次のように記述されている。

l1: cid ⊇ 1 ∨ cid ⊇ 2

これにより、利用権r1はコンテンツc1とc2に対応する。即ち、利用権r1を保有している端末では、コンテンツc1とc2を利用する事ができる。

ライセンス12の属性条件は、次のように記述されている。

l2: aid ⊇ 0 ∧ (2001年1月1日 < reldate < 2001年12月31日)

これは、2001年にリリースされた0番のアーティストのコンテンツ、という意味の条件であり、ライセンス12はコンテンツc3とc4に対応する。この時点で、ライセンス12を保有している端末では、コンテンツc3とc4を利用する事ができる。後に下記のような属性情報を持たせたコンテンツc5が発行されたとする。

c5: cid = {5}, aid = {0}, reldate = {2001年12月1日}

このコンテンツをコンテンツサーバ3からダウンロードするなどして入手すると、既にライセンス12を保有しているクライアント1では、新たにライセンスサーバ等に接続する必要なく、コンテンツc5も利用できるようになる。

これらのコンテンツの配布後、配信事業者が新たにベスト版としてコンテンツc1, c2, c5を組み合わせて発売しようとするならば、それに対応する次のようなライセンス13を発行すれば、コンテンツを新たに作成する必要なく、配布済み・流通中のコンテンツをそのまま活用して、ベスト版発売が可能である。

13: cid ∋ 1 ∨ cid ∋ 2 ∨ cid ∋ 5

このようにして、配布済み・流通中のコンテンツを組み合わせた利用権を容易に新規発行できる。例えば、リリース日とアーティストを制約した属性条件を持つライセンスを発行することで、あるアーティストの特定の年代にリリースされた作品を含む全集を新たに発売することができる。

また、アーティストを制約した属性条件を持つライセンスを発行することで、あるグループの全集（グループによる作品、グループのメンバーのソロ作品などを含む）を新たに発売することができる。

次に、サブスクリプション・サービスとして、毎月いくつかの新譜を追加利用できるようになるライセンスを定義する例を示す。

ライセンス 14 の属性の条件を、次のように定義する。

14: cid ∋ 3 ∨ cid ∋ 4 ∨ sid ∋ 1

このライセンス 14 を所持しているクライアント 1 では、まず、既に発行されているコンテンツ c3 と c4 が利用可能である。翌月、新譜として次のような属性情報を持ったコンテンツ c6 と c7 が発行されたとする。

c6: cid = {6}, sid = {1}

c7: cid = {7}, sid = {1}

この場合、ライセンス 14 を持っているクライアント 1 は、新たにライセンスを購入する必要なく、コンテンツ c6 と c7 を利用する事ができる。同様にして、月ごとにサブスクリプション ID に 1 を含んだコンテンツを発行する事により、ライセンス 14 を持っているクライアント 1 はライセンスを別途購入することなく、利用可能なコンテンツを追加していく事ができる。

このように、属性条件を属性項目、属性値、及び論理演算子、関係演算子等の演算子の組み合わせで表すことで、利用できるコンテンツの集合を柔軟に設定できるようになる。

属性条件に含まれる演算子はここに挙げられているに限定されず、その他の各種演算子を利用することができる。

図８を参照して、クライアント１がコンテンツを再生する場合の処理について説明する。

ステップＳ４１において、クライアント１のCPU２１は、ユーザが入力部２６を操作することで指示したコンテンツIDを取得する。

そして、CPU２１は、コンテンツIDを取得すると該当するコンテンツデータのヘッダに記述されている属性情報を読み取る。

次に、ステップＳ４２に進み、CPU２１は、ステップＳ４１で読み取られた属性情報が各ライセンスに記述されている属性条件を満たすライセンスが、クライアント１により既に取得され、記憶部２８に記憶されているか否かを判定する。そのようなライセンスが見つからなかった場合には、ステップＳ４３に進み、ＣＰＵ２１は、出力部２７を介して、ディスプレイにライセンスの取得を促すメッセージを表示する。

ステップＳ４２において、ライセンスが既に取得されていると判定された場合、ステップＳ４４に進み、CPU２１は、取得されているライセンスは有効期限内のものであるか否かを判定する。ライセンスが有効期限内のものであるか否かは、ライセンスの内容として規定されている期限と、タイマ２０により計時されている現在日時と比較することがで判断される。ライセンスの有効期限が既に満了していると判定された場合、CPU２１は、ステップＳ４５に進み、ライセンス更新処理を実行する。このライセンス更新処理の詳細は、図８のフローチャートを参照して後述する。

ステップＳ４４において、ライセンスはまだ有効期限内であると判定された場合、または、ステップＳ４５において、ライセンスが更新された場合、ステップＳ４５に進み、CPU２１は、コンテンツのヘッダに含まれる電子署名及びライセンスに含まれる電子署名をライセンスサーバ４の公開鍵で検証する。電子署名の検証の結果、電子署名が正しいと判断された場合、ステップＳ４６に進み、CPU２１は、暗号化されているコンテンツデータを記憶部２８から読み出し、RAM２３に格納させる。そして、ステップＳ４７において、CPU２１は、RAM２３に記

憶された暗号化ブロックのデータを、図５のデータに配置されている暗号化ブロック単位で、暗号化復号部２４に供給し、復号させる。

CPU２１は、さらに、ステップＳ４８において、暗号化復号部２４により復号されたコンテンツデータをコーデック部２５に供給し、デコードさせる。そして、コーデック部２５によりデコードされたデータを、CPU２１は、入出力インタフェース３２から出力部２７に供給し、D/A 変換させ、スピーカから出力させる。

図９乃至図 11 を用いてクライアントがライセンスサーバ４からライセンスを取得する処理を説明する。

図９はクライアント１のユーザが利用したいコンテンツが決まっている場合のライセンス取得処理を示している。ユーザが、入力部２６を操作することでコンテンツを指定しライセンスサーバ４にライセンスリストの要求を指示すると、CPU２１は、通信部２９を制御し、インターネット２を介してコンテンツサーバ３に指定されたコンテンツのコンテンツ ID を含むライセンスリスト要求を送信する。ライセンスサーバ４はライセンスリスト要求を受信すると、受信したライセンスリストに含まれるコンテンツ ID から、該当するコンテンツを利用可能なライセンスを抽出し、各ライセンスのライセンス ID、ライセンス名、利用できるコンテンツの条件、現在利用できるコンテンツのリスト、コンテンツの使用条件等を記載したライセンスリストをクライアント１に送信する。

クライアント１がライセンスサーバ４からライセンスリストを受信すると、CPU２１は、出力部２７にライセンスリストに含まれる各ライセンスの情報を表示する。ユーザがその情報を参照し、所望するライセンスを選択すると、CPU２１は、通信部２９を制御し、SSL などの相互認証によりセッションを形成した後、インターネット２を介してコンテンツサーバ３に、選択されたライセンスのライセンス ID と端末 ID と課金用のユーザ ID 及びパスワードを含むライセンス要求を暗号化して送信する。ライセンスサーバ４はクライアント１から送信されたライセンス要求を受信すると、後述するライセンス発行処理を行った後、ライセンス要求に含まれるライセンス ID に対応するライセンスをクライアント１に送信

する。クライアント１はライセンスサーバ４から送信されたライセンスを受信すると、受信したライセンスを暗号化等をしてセキュアな状態で記憶部２８に保存する。

以上のようにして、ユーザはクライアント１が既に所持しているコンテンツを利用するためのライセンスを取得することができる。以上のライセンス取得処理は、ユーザがクライアントに所持しているコンテンツを再生する操作した際に、そのコンテンツを再生するためのライセンスを取得していなかった場合、自動的に開始されるようにしても良い。

次に、ユーザが各種検索条件を指定してライセンスを検索し、取得する処理を図１６に示す。まず、ユーザが欲しいライセンスを検索するための、ライセンス名、ライセンスの種類、ライセンスが利用可能とするコンテンツのタイトル、アルバム名、ジャンル、アーティスト名、リリース日等の検索条件を入力部２６を操作することによって指定すると、CPU２１は、通信部を制御し、入力された検索条件をフォーマットしたデータを含むライセンスリスト要求をコンテンツサーバ３に送信する。コンテンツサーバはクライアント１から送信されたライセンスリスト要求を受信すると、ライセンスリスト要求に含まれる検索条件を満たすライセンスを記憶部２８から検索し、ライセンス ID 等の各ライセンスに関する情報を含むライセンスリストをクライアント１に送信する。

クライアント１がライセンスサーバ４からライセンスリストを受信すると、CPU２１は、出力部２７にライセンスリストに含まれる各ライセンスの情報を表示する。ユーザがその情報を参照し、所望するライセンスを選択すると、CPU２１は、通信部２９を制御し、SSL などの相互認証によりセッションを形成した後、インターネット２を介してコンテンツサーバ３に、選択されたライセンスのライセンス ID と端末 ID と課金用のユーザ ID 及びパスワードを含むライセンス要求を暗号化して送信する。ライセンスサーバ４はクライアント１から送信されたライセンス要求を受信すると、後述するライセンス発行処理を行った後、ライセンス要求に含まれるライセンス ID に対応するライセンスをクライアント１に送信

する。クライアント１はライセンスサーバ４から送信されたライセンスを受信すると、受信したライセンスを暗号化するなどしてセキュアな状態で記憶部２８に保存する。

以上のようにして、ユーザは欲しいライセンスを検索し、取得することができる。

次に、ユーザが欲しいライセンスのライセンス ID を知っている場合のライセンス取得処理を図 11 に示す。

ユーザがライセンス ID を入力部２６を操作し入力して、欲しいライセンスのライセンス ID を指定すると、CPU２１は、通信部２９を制御し、SSL などの相互認証によりセッションを形成した後、インターネット２を介してコンテンツサーバ３に、選択されたライセンスのライセンス ID と端末 ID と課金用のユーザ ID 及びパスワードを含むライセンス要求を暗号化して送信する。ライセンスサーバ４はクライアント１から送信されたライセンス要求を受信すると、後述するライセンス発行処理を行った後、ライセンス要求に含まれるライセンス ID に対応するライセンスをクライアント１に送信する。クライアント１はライセンスサーバ４から送信されたライセンスを受信すると、受信したライセンスを暗号化等をしてセキュアな状態で記憶部２８に保存する。

以上のようにして、ユーザは雑誌などに記載されているライセンスの広告などからライセンス ID を知り、そのライセンス ID を指定することで所望するライセンスを取得することができる。

また、Web サイトの HTML ファイルや電子メール等にライセンスＩＤを含むライセンスサーバの URL のリンク情報が記載されており、これをユーザがクリックするなどして選択することでライセンス取得処理を開始するようにしても良い。

図 12 のフローチャートを参照して、図９乃至図 11 におけるライセンス発行処理の詳細を説明する。なお、この場合においても、図２のクライアント１の構成は、ライセンスサーバ４の構成としても引用される。

最初にステップＳ１０２において、CPU２１はライセンス要求に含まれるライセンスID、端末ID、ユーザID、パスワードを取り込む。

そして、ライセンスサーバ４のCPU２１は、通信部２９から課金サーバ５にアクセスし、ユーザIDとパスワードに対応するユーザの与信処理を要求する。課金サーバ５は、インターネット２を介してライセンスサーバ４から与信処理の要求を受けると、そのユーザIDとパスワードに対応するユーザの過去の支払い履歴などを調査し、そのユーザが、過去にライセンスの対価の不払いの実績があるか否かなどを調べ、そのような実績がない場合には、ライセンスの付与を許容する与信結果を送信し、不払いの実績などがある場合には、ライセンス付与の不許可の与信結果を送信する。

ステップＳ１０４において、ライセンスサーバ４のCPU２１は、課金サーバ５からの与信結果が、ライセンスを付与することを許容する与信結果であるか否かを判定し、ライセンスの付与が許容されている場合には、ステップＳ１０５に進み、ライセンスIDに対応するライセンスをデータベースから取り出し、ライセンスの使用規則のフィールドに端末IDを挿入し、ライセンスサーバ４の秘密鍵で電子署名を生成、付加する。

そして、ステップＳ１０７に進み、ライセンスサーバ４のCPU２１は、その端末IDと電子署名が付加されたライセンスを通信部２９からインターネット２を介してクライアント１に送信させる。

ステップＳ１０８においてライセンスサーバ４のCPU２１は、ステップＳ１０７の処理で、いま送信したライセンスをステップＳ１０２の処理で取り込まれたユーザIDとパスワードに対応して、記憶部２８に記憶させる。さらに、ステップＳ１０９において、CPU２１は、課金処理を実行する。具体的には、CPU２１は、通信部２９から課金サーバ５に、そのユーザIDとパスワードに対応するユーザに対する課金処理を要求する。課金サーバ５は、この課金の要求に基づいて、そのユーザに対する課金処理を実行する。上述したように、この課金処理に対して、そのユーザが支払いを行わなかったような場合には、以後、そのユーザは、

ライセンスの付与を要求したとしても、ライセンスを受けることができないことになる。

すなわち、この場合には、課金サーバ５からライセンスの付与を不許可とする与信結果が送信されてくるので、ステップＳ１０４からステップＳ１１０に進み、CPU２１は、エラー処理を実行する。具体的には、ライセンスサーバ４のCPU２１は、通信部２９を制御してアクセスしてきたクライアント１に対して、ライセンスを付与することができない旨のメッセージを出力し、処理を終了させる。

この場合、上述したように、そのクライアント１はライセンスを受けることができないので、そのコンテンツを利用することができないことになる。

次に、図１３を用いてライセンスが利用可能なコンテンツのコンテンツデータを取得する処理を説明する。

ユーザが入力部２６を操作し、ライセンスを選択すると、CPUは、通信部２９を制御し、インターネット２を介してコンテンツサーバ３に、選択されたライセンスのライセンスIDを含むコンテンツリスト要求を送信する。ライセンスサーバ４はコンテンツリスト要求を受信すると、コンテンツリスト要求に含まれるライセンスIDを取り出す。ライセンスサーバ４はライセンスIDをキーとしてライセンスデータベースから、該当するライセンスによって利用可能なコンテンツを抽出する。その後、ライセンスサーバは、抽出された各コンテンツのコンテンツID、コンテンツをダウンロードするためのURL、及びコンテンツ名、アーティスト名、ジャンル等のコンテンツ情報を含む、コンテンツリストをクライアント１に送信する。

クライアント１は出力部を制御してコンテンツリストを受信するとコンテンツリストに含まれる各コンテンツのコンテンツ情報を表示させる。ユーザが表示されたコンテンツ情報を参照して、ダウンロードするコンテンツを選択すると、クライアント１はコンテンツのURLに従って、コンテンツサーバにコンテンツ要求をコンテンツサーバ３に送信する。コンテンツサーバはコンテンツ要求を受信すると、コンテンツ要求に含まれるコンテンツIDを持つコンテンツをクライア

ント１に送信する。クライアント１はコンテンツサーバ３からコンテンツを受信すると、受信したコンテンツを記憶部２８に記憶させる。

以上のようにして、ユーザはライセンスにより利用可能となるコンテンツを探し出し、コンテンツサーバ３からクライアントのダウンロードさせることができる。

図１４は、ブロードキャストインクリプション（Broadcast Encryption）を、キーの管理方式に採用した場合におけるキーの構成方法を表している。図１４に示されるように、キーは、階層ツリー構造とされ、最下段のリーフ（leaf）が個々のデバイスに対応する。図１４の例の場合、番号０から番号１５までの１６個のデバイスに対応するキーが生成される。

各キーは、図中丸印で示される各ノードに対応して規定される。この例では、最上段のルートノードに対応してキーＫＲが、２番目のノードに対応してキーＫ０，Ｋ１が、３段目のノードに対応してキーＫ００乃至Ｋ１１が、第４番目のノードに対応してキーＫ０００乃至キーＫ１１１が、それぞれ対応されている。そして、最下段のノードとしてのリーフ（デバイスノード）に、キーＫ００００乃至Ｋ１１１１が、それぞれ対応されている。

階層構造とされているため、例えば、キーＫ００１０とキー００１１の上位のキーは、Ｋ００１とされ、キーＫ０００とキーＫ００１の上位のキーは、Ｋ００とされている。以下同様に、キーＫ００とキーＫ０１の上位のキーは、Ｋ０とされ、キーＫ０とキーＫ１の上位のキーは、ＫＲとされている。

コンテンツを利用するために用いるキーは、最下段のデバイスノード（リーフ）から、最上段のルートノードまでの１つのパスの各ノードに対応するキーで構成される。例えば、番号３のコンテンツを利用するキーは、キーＫ００１１，Ｋ００１，Ｋ００，Ｋ０，ＫＲを含むリーフからルートまでのパス上の各キーで構成される。

本発明のシステムにおいては、例えば、図１５に示されるように、８×２４×３２段のノードに対応するキーで構成される階層ツリー構造キーシステムが利用

される。このキーシステムでは、ルートノードから下位の８段までの各ノードに対応するキーに、カテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。

図１５の例では、ルートノードから８段目のノードのうちの１つのノードに、本発明のシステムが対応される。このノードよりさらに下の階層の２４段のノードに対応するキーにより、ライセンスが対応される。これにより、約１６メガ（＝$2^{24}$＝約１６０万）のライセンスを規定することができる。さらに、最も下側の３２段の階層により、約４ギガ（＝$2^{32}$＝約４０億）のユーザを規定することができる。最下段の３２段のノードに対応するキーが、DNK（Device Node Key）を構成する。

各コンテンツは、６４（＝８＋２４＋３２）段の各ノードで構成されるパスの内の１つに対応される。すなわち、各コンテンツの暗号化には、割り当てられたパスを構成するノードに対応するキーが用いられる。上位の階層のキーは、その直近の下位の階層のキーを用いて暗号化され、図５のＥＫＢ内に配置される。最下段のＤＮＫは、ＥＫＢ内には配置されず、クライアントがライセンスサーバに登録するときに取得するサービスデータに記述され、図１６に示されるように、ユーザのクライアント１に与えられる。

クライアント１は、サービスデータに記述されているＤＮＫを用いて、コンテンツデータとともに配布されるＥＫＢ内に記述されている直近の上位の階層のキーを復号し、復号して得たキーを用いて、ＥＫＢ内に記述されているさらにその上の階層のキーを復号する。以上の処理を順次行うことで、クライアント１は、そのコンテンツのパスに属するすべてのキーを得ることができる。

クライアント１は以上のEKBの復号処理を行った後得られるKRを用いて、KRによって暗号化されているコンテンツキーKR(KC)を復号し、コンテンツキーKCを得ることができる。

なお、本発明におけるキーは、図１４および図１５に示されるようなブロードキャストインクリプションを利用したキーシステム以外のキーで構成することも可能である。

また、本発明が適用されるクライアントは、いわゆるパーソナルコンピュータ以外に、PDA（Personal Digital Assistants）、携帯電話機、ゲーム端末機などとすることができる。

一連の処理をソフトウエアにより実行させる場合には、そのソフトウエアを構成するプログラムが、専用のハードウエアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

この記録媒体は、図２に示すように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク４１（フロッピディスクを含む）、光ディスク４２（CD-ROM(Compact Disk-Read Only Memory),DVD(Digital Versatile Disk)を含む）、光磁気ディスク４３（MD（Mini-Disk）を含む）、もしくは半導体メモリ４４などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM２２や、記憶部２８に含まれるハードディスクなどで構成される。

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

産業上の利用可能性

以上の如く、本発明の情報処理装置および方法、プログラム格納媒体、並びにプログラムによれば、暗号化されたデータとコンテンツの属性情報を、所定のフォーマットにフォーマット化して、出力するようにし、ライセンスに属性条件を含むようにし、コンテンツの属性情報がライセンスの属性条件を満たす場合に暗号化されたデータを復号できるようにしたので、データが不正に利用されるのを抑制しつつ、ライセンスを柔軟に発行することが可能となる。

請求の範囲

1． 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信手段と、

前記コンテンツを記憶するコンテンツ記憶手段と、

利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信手段と、

前記ライセンスを記憶するライセンス記憶手段と、

前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを判定する判定手段と、

前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号手段と、

前記復号手段により復号されたコンテンツデータを出力する出力手段と

を備えることを特徴とする情報処理装置。

2． 前記コンテンツは、更に前記コンテンツデータを復号するためのコンテンツキーを含む

ことを特徴とする請求の範囲第1項に記載の情報処理装置。

3． 前記属性情報は、属性項目と属性値の組み合わせからなる

ことを特徴とする請求の範囲第1項に記載の情報処理装置。

4． 前記属性項目はレコード会社、アーティスト、リリース日、コンテンツ発行者、ジャンル、サブスクリプション、またはレーベルに関する情報を含む

ことを特徴とする請求の範囲第1項に記載の情報処理装置。

5． 前記属性条件は属性項目、属性値、及び演算子の組み合わせからなる

ことを特徴とする請求の範囲第1項に記載の情報処理装置。

6． コンテンツに含まれる属性情報に関する条件を記載した属性条件を含むライセンスを一意に識別するライセンス ID を含むライセンス要求を受信する受信手段と、

ライセンスをライセンスIDと共に記憶する記憶手段と、

前記ライセンス要求に含まれる前記ライセンスIDに対応する前記ライセンスを取り込む取り込み手段と、

前記ライセンスに電子署名を付加する署名手段と、

署名手段により署名されたライセンスを送信する送信手段と

を備えることを特徴とする情報処理装置。

7. 更に、前記取り込み手段によって取り込まれたライセンスに端末IDを付加するライセンス処理手段

を備えることを特徴とする請求の範囲第6項に記載の情報処理装置。

8. 暗号化コンテンツデータと属性情報とを含むコンテンツを記憶する記憶手段と、

コンテンツを一意に識別するコンテンツIDを含むコンテンツ要求を受信する受信手段と、

コンテンツ要求に含まれるコンテンツIDに対応するコンテンツを送信する送信手段と

を備える情報処理装置であって、

前記コンテンツに含まれる前記属性情報は、当該コンテンツを利用する際にライセンスの属性条件を満たすか否かを判断するために用いられる情報であり、

前記ライセンスの属性条件は利用できる前記コンテンツの前記属性情報に関する条件を記載した情報である

ことを特徴とする情報処理装置。

9. 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、

前記コンテンツを記憶するコンテンツ記憶ステップと、

利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、

前記ライセンスを記憶するライセンス記憶ステップと、

前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを判定する判定ステップと、

前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、

前記復号手段により復号されたコンテンツデータを出力する出力ステップと

を含むことを特徴とする情報処理方法。

１０．　暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、

前記コンテンツを記憶するコンテンツ記憶ステップと、

利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、

前記ライセンスを記憶するライセンス記憶ステップと、

前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを判定する判定ステップと、

前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、

前記復号手段により復号されたコンテンツデータを出力する出力ステップと

をコンピュータに実行させるプログラム。

１１．　暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、

前記コンテンツを記憶するコンテンツ記憶ステップと、

利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、

前記ライセンスを記憶するライセンス記憶ステップと、

前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているラ

イセンスの属性条件を満たすか否かを判定する判定ステップと、

前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、

前記復号手段により復号されたコンテンツデータを出力する出力ステップと

をコンピュータに実行させるプログラムが格納されたプログラム格納媒体。

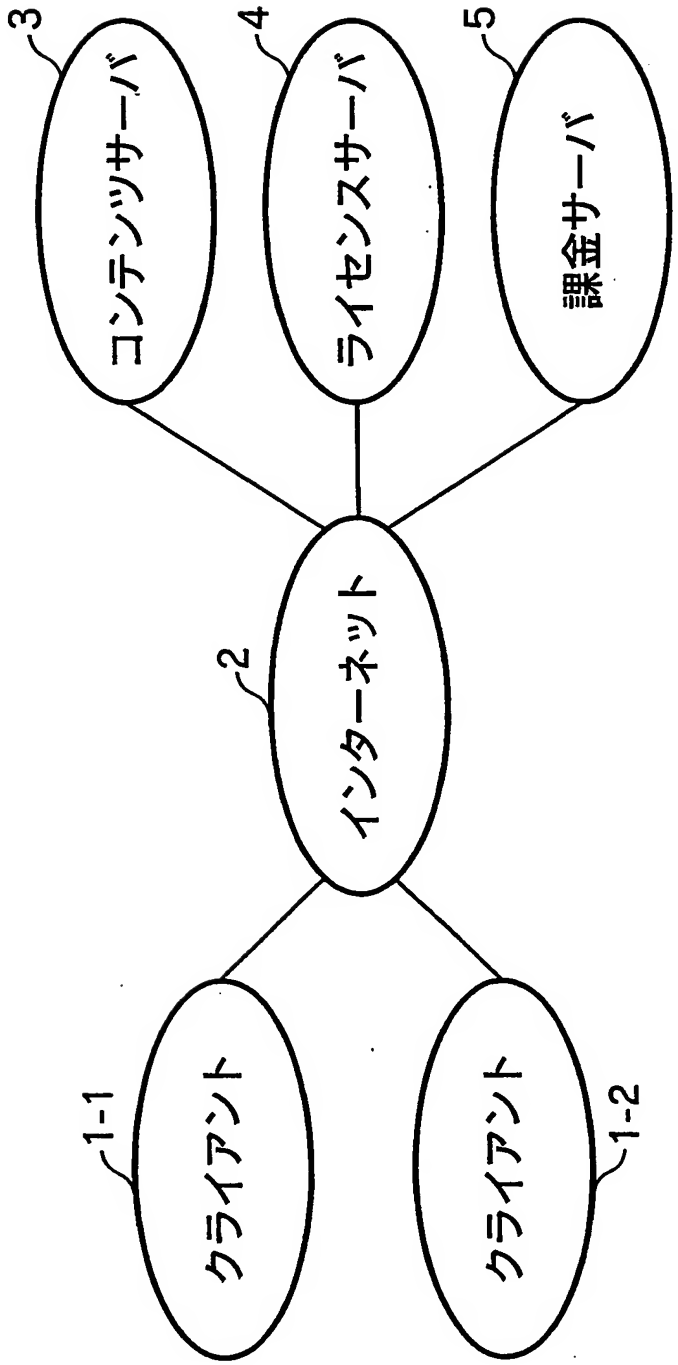



図1

図2

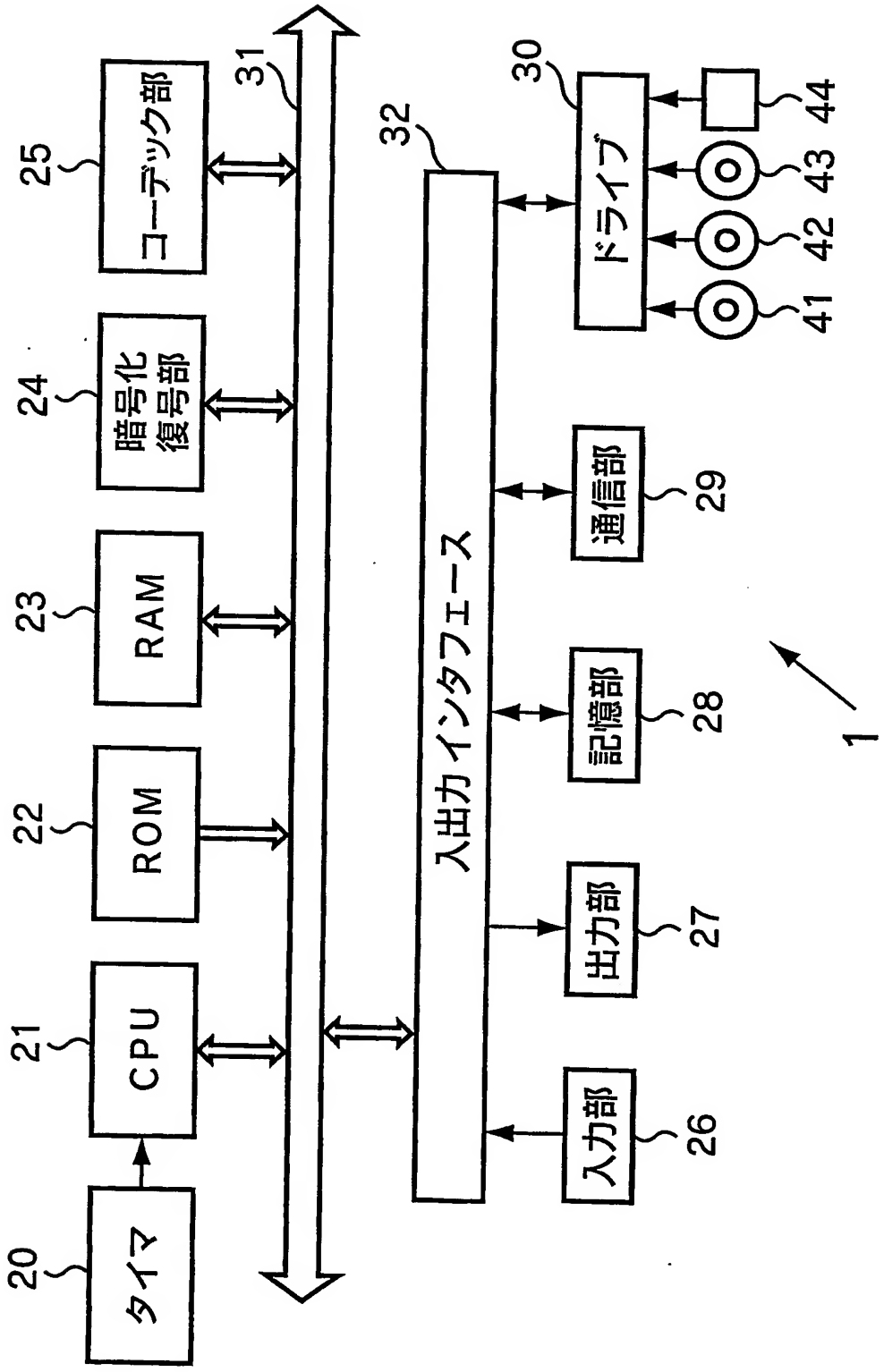

タイマ
20
CPU
21
ROM
22
RAM
23
暗号化復号部
24
コーデック部
25
31
入力部
26
出力部
27
記憶部
28
通信部
29
入出力インタフェース
32
ドライブ
30
41
42
43
44
1

図3

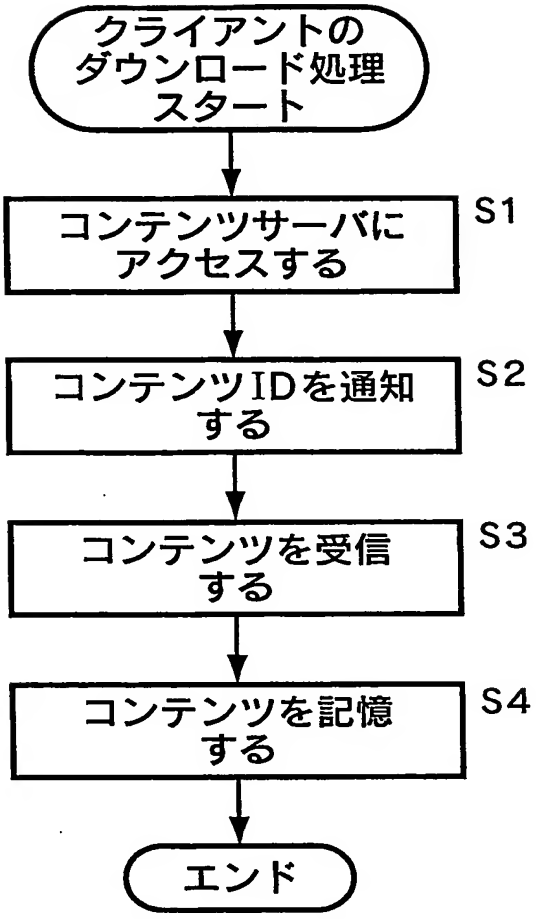

クライアントの
ダウンロード処理
スタート
コンテンツサーバに
アクセスする
S1
コンテンツIDを通知
する
S2
コンテンツを受信
する
S3
コンテンツを記憶
する
S4
エンド

図4

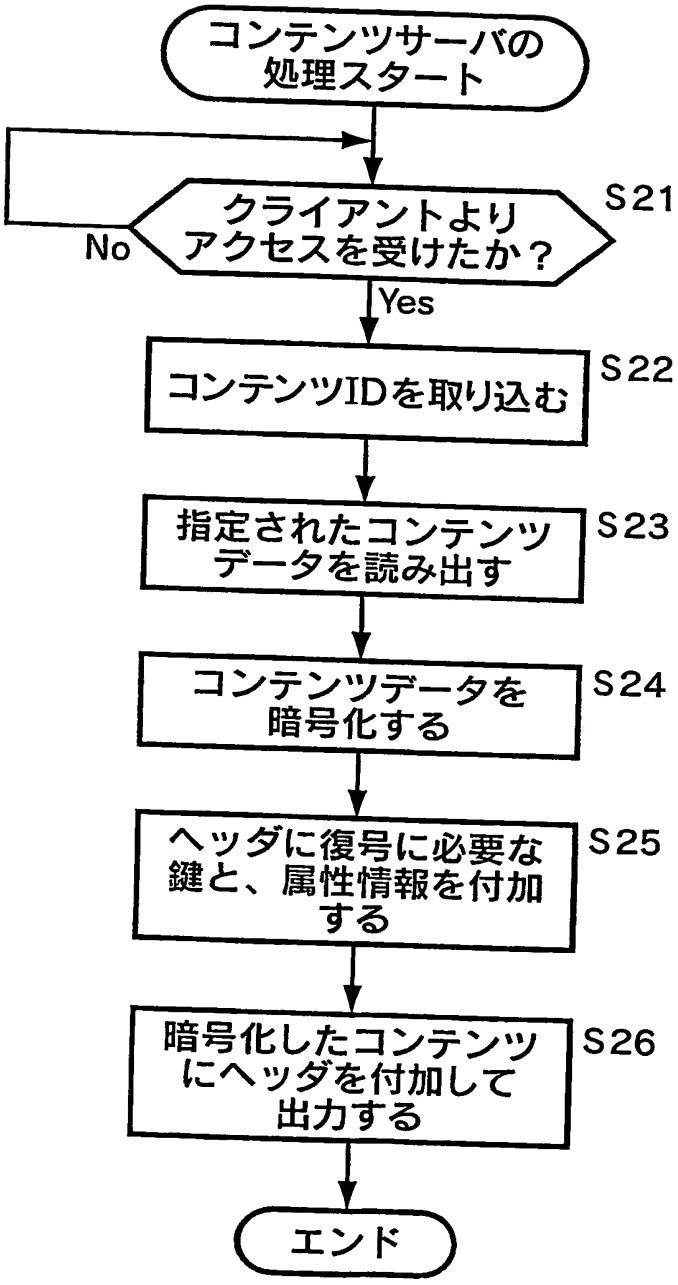

コンテンツサーバの処理スタート
クライアントよりアクセスを受けたか？
S21
No
Yes
コンテンツIDを取り込む
S22
指定されたコンテンツデータを読み出す
S23
コンテンツデータを暗号化する
S24
ヘッダに復号に必要な鍵と、属性情報を付加する
S25
暗号化したコンテンツにヘッダを付加して出力する
S26
エンド

図5

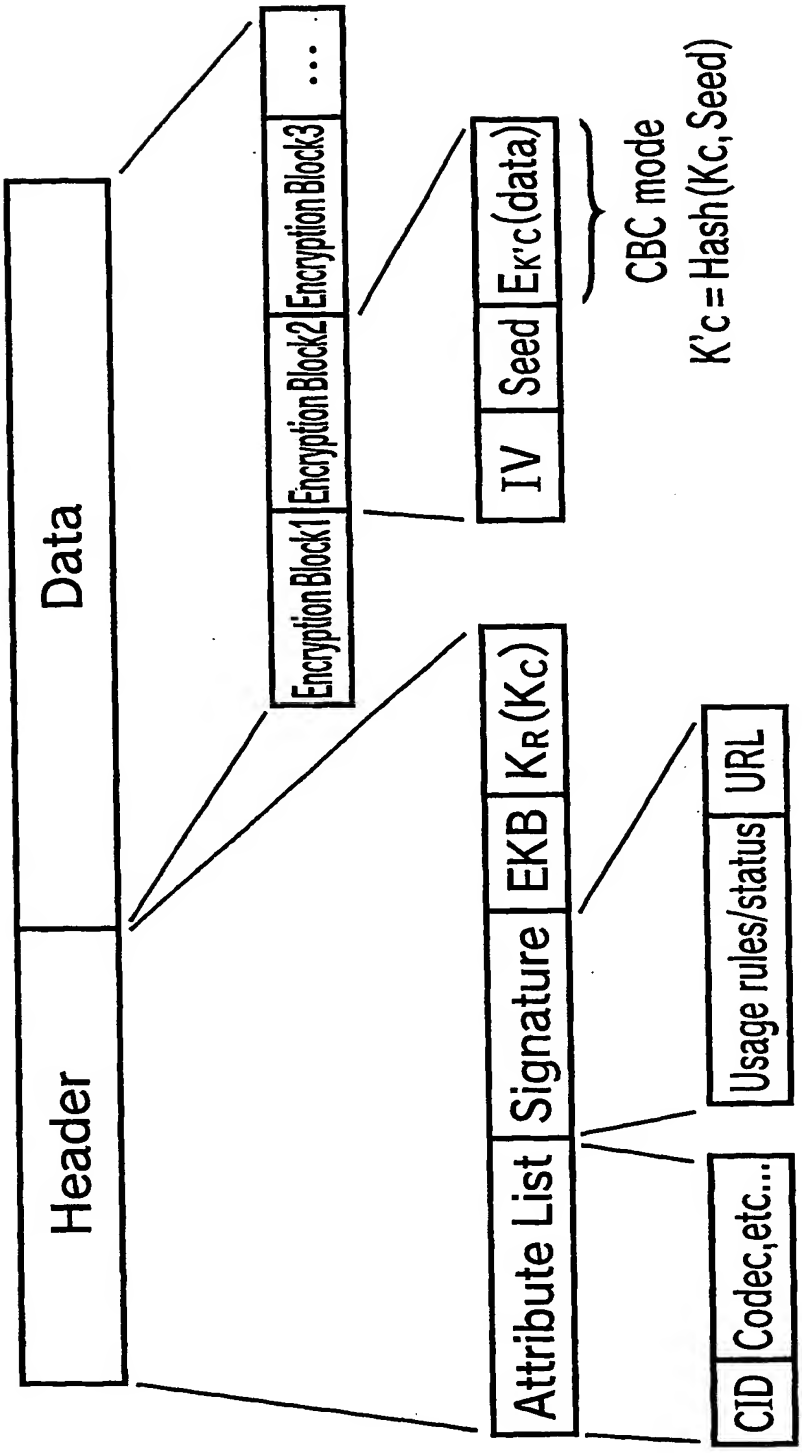

Header
Data
Attribute List
Signature
EKB
KR(Kc)
CID
Codec,etc...
Usage rules/status
URL
Encryption Block1
Encryption Block2
Encryption Block3
...
IV
Seed
EK'c(data)
CBC mode
K'c = Hash(Kc, Seed)

図6

| 属性項目 | 説明 |
|---|---|
| CID | コンテンツID |
| RCID | レコード会社ID |
| CIID | コンテンツ発行者ID |
| AID | アーティストID |
| RelDate | リリース日 |
| GID | ジャンルID |
| LID | レーベルID |
| SID | サブスクリプションID |
| URL | ライセンスサーバのURL |

図7

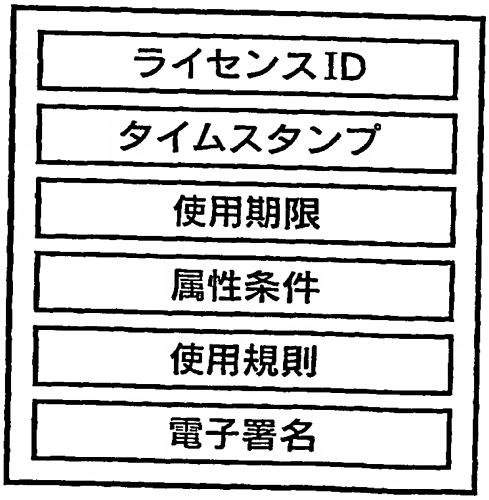


図8

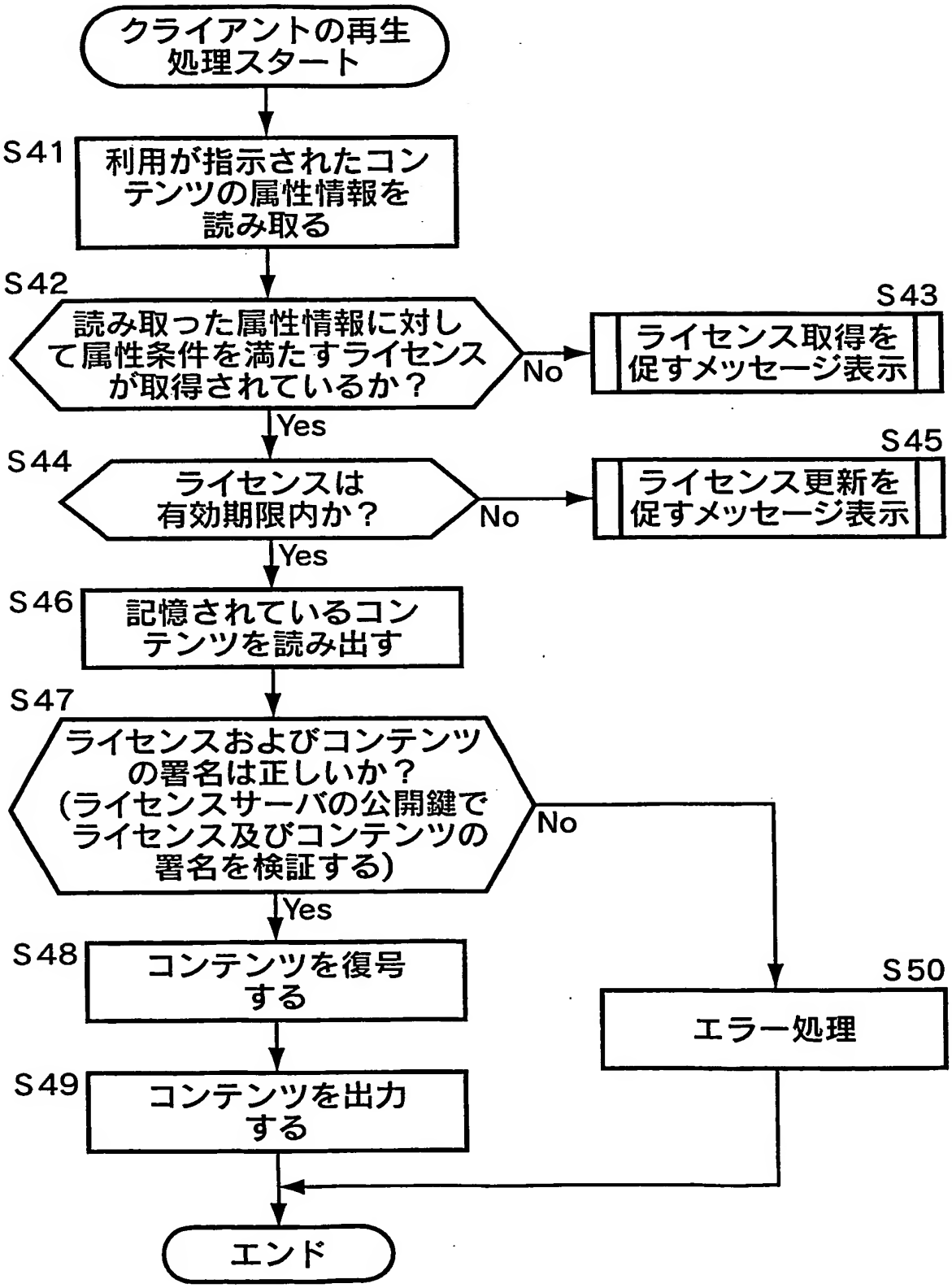

クライアントの再生処理スタート
S41
利用が指示されたコンテンツの属性情報を読み取る
S42
読み取った属性情報に対して属性条件を満たすライセンスが取得されているか？
No
S43
ライセンス取得を促すメッセージ表示
Yes
S44
ライセンスは有効期限内か？
No
S45
ライセンス更新を促すメッセージ表示
Yes
S46
記憶されているコンテンツを読み出す
S47
ライセンスおよびコンテンツの署名は正しいか？(ライセンスサーバの公開鍵でライセンス及びコンテンツの署名を検証する)
No
Yes
S48
コンテンツを復号する
S49
コンテンツを出力する
S50
エラー処理
エンド

図9

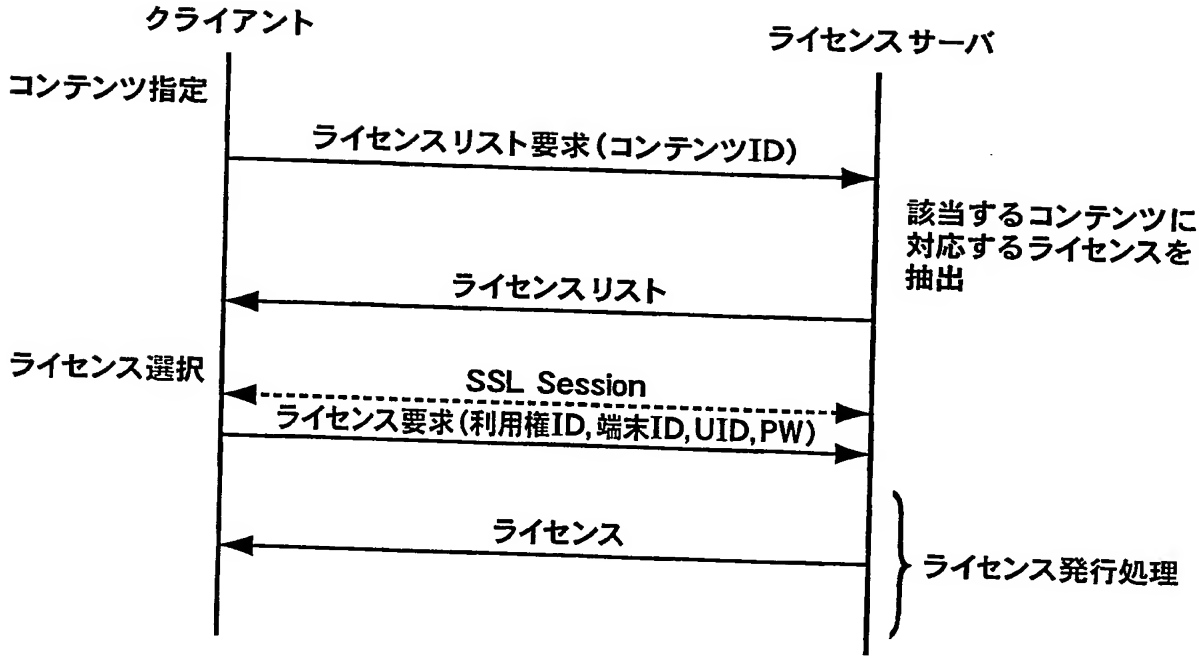

クライアント
ライセンスサーバ
コンテンツ指定
ライセンスリスト要求(コンテンツID)
該当するコンテンツに
対応するライセンスを
抽出
ライセンスリスト
ライセンス選択
SSL Session
ライセンス要求(利用権ID,端末ID,UID,PW)
ライセンス
ライセンス発行処理

図10

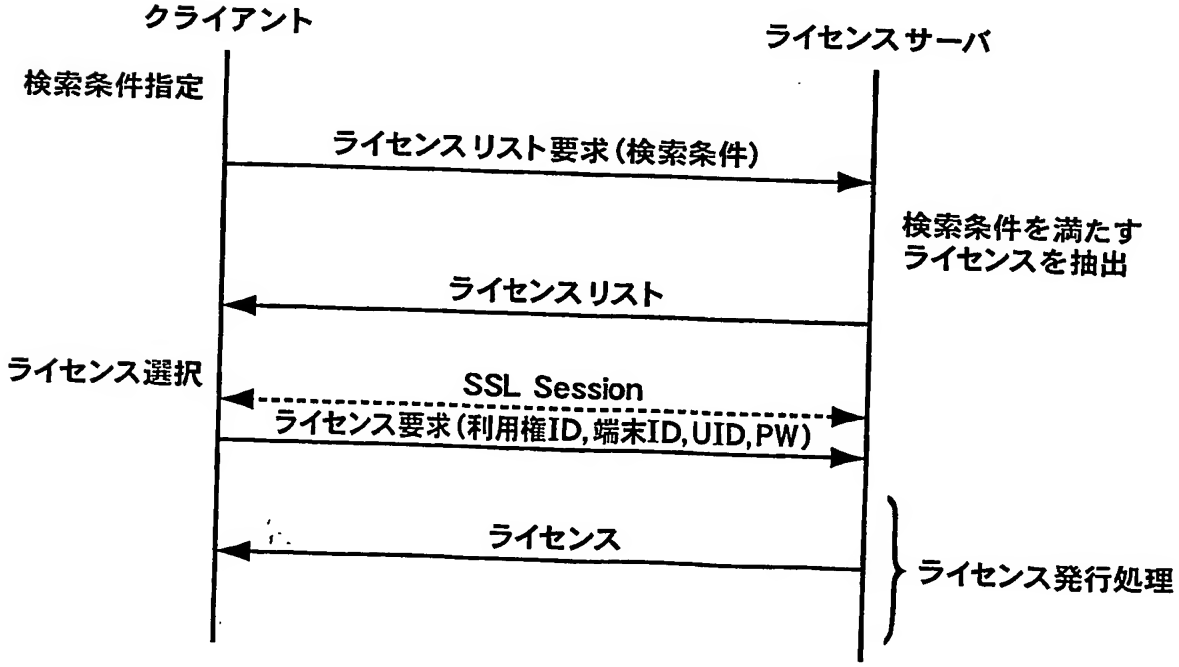

クライアント
ライセンスサーバ
検索条件指定
ライセンスリスト要求(検索条件)
検索条件を満たす
ライセンスを抽出
ライセンスリスト
ライセンス選択
SSL Session
ライセンス要求(利用権ID,端末ID,UID,PW)
ライセンス
ライセンス発行処理

図11

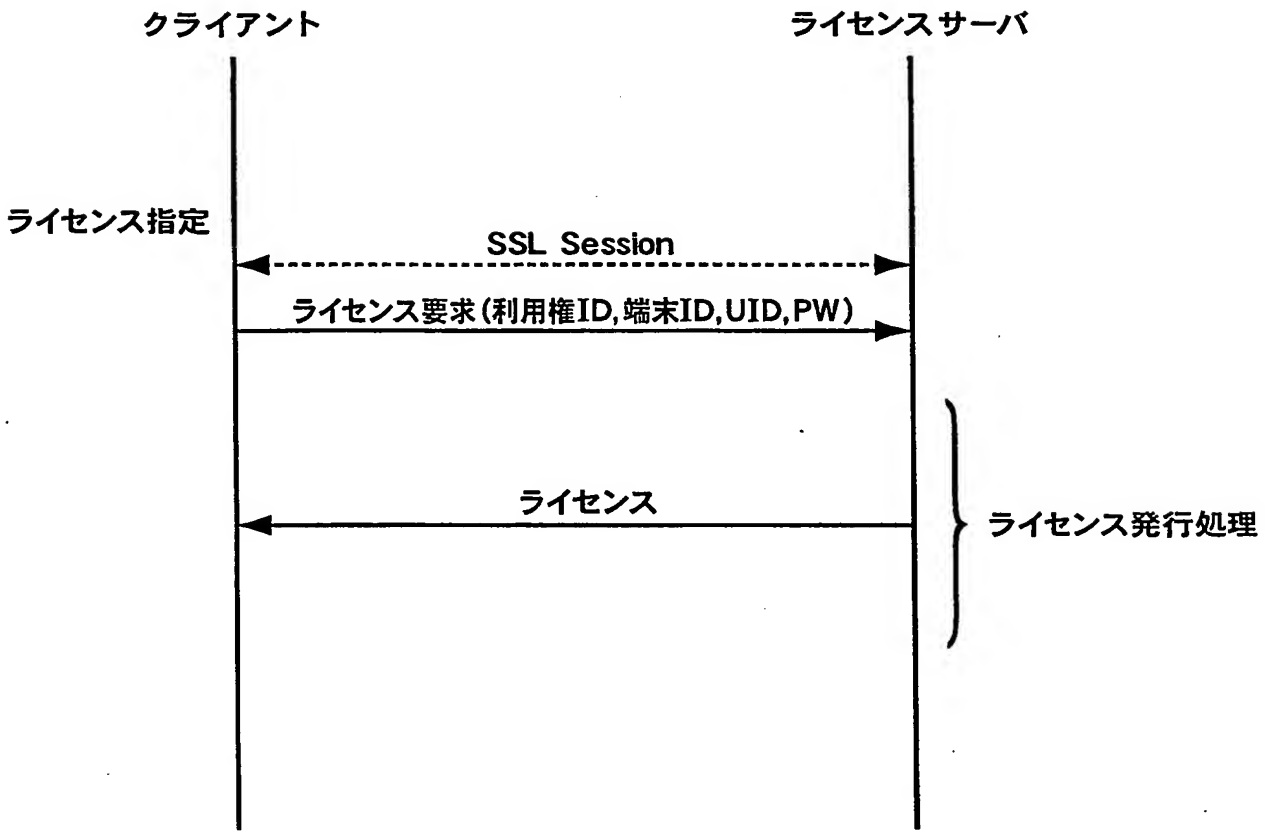

クライアント
ライセンスサーバ
ライセンス指定
SSL Session
ライセンス要求(利用権ID,端末ID,UID,PW)
ライセンス
ライセンス発行処理

図12

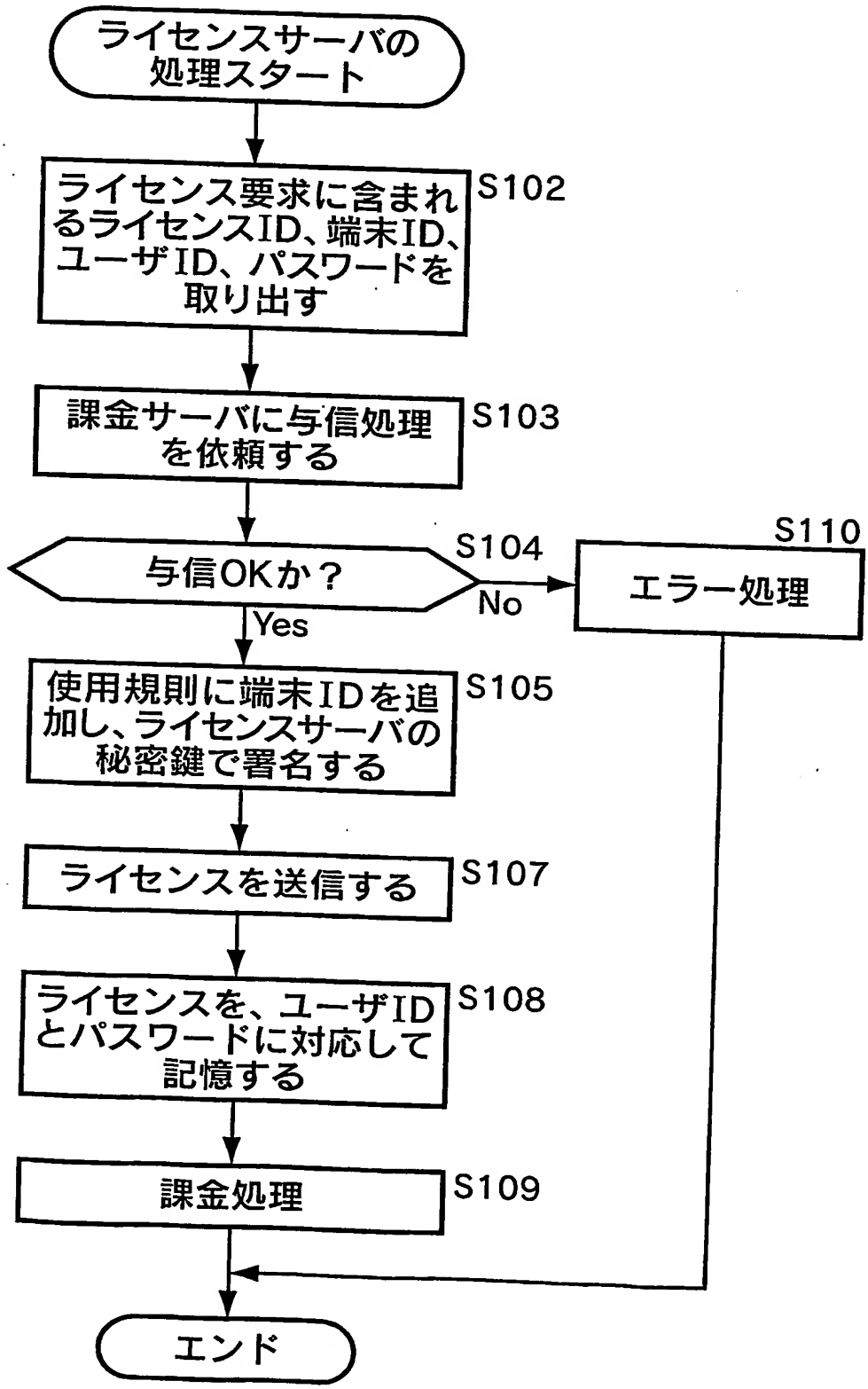

ライセンスサーバの処理スタート
ライセンス要求に含まれるライセンスID、端末ID、ユーザID、パスワードを取り出す
S102
課金サーバに与信処理を依頼する
S103
与信OKか？
S104
No
エラー処理
S110
Yes
使用規則に端末IDを追加し、ライセンスサーバの秘密鍵で署名する
S105
ライセンスを送信する
S107
ライセンスを、ユーザIDとパスワードに対応して記憶する
S108
課金処理
S109
エンド

図13

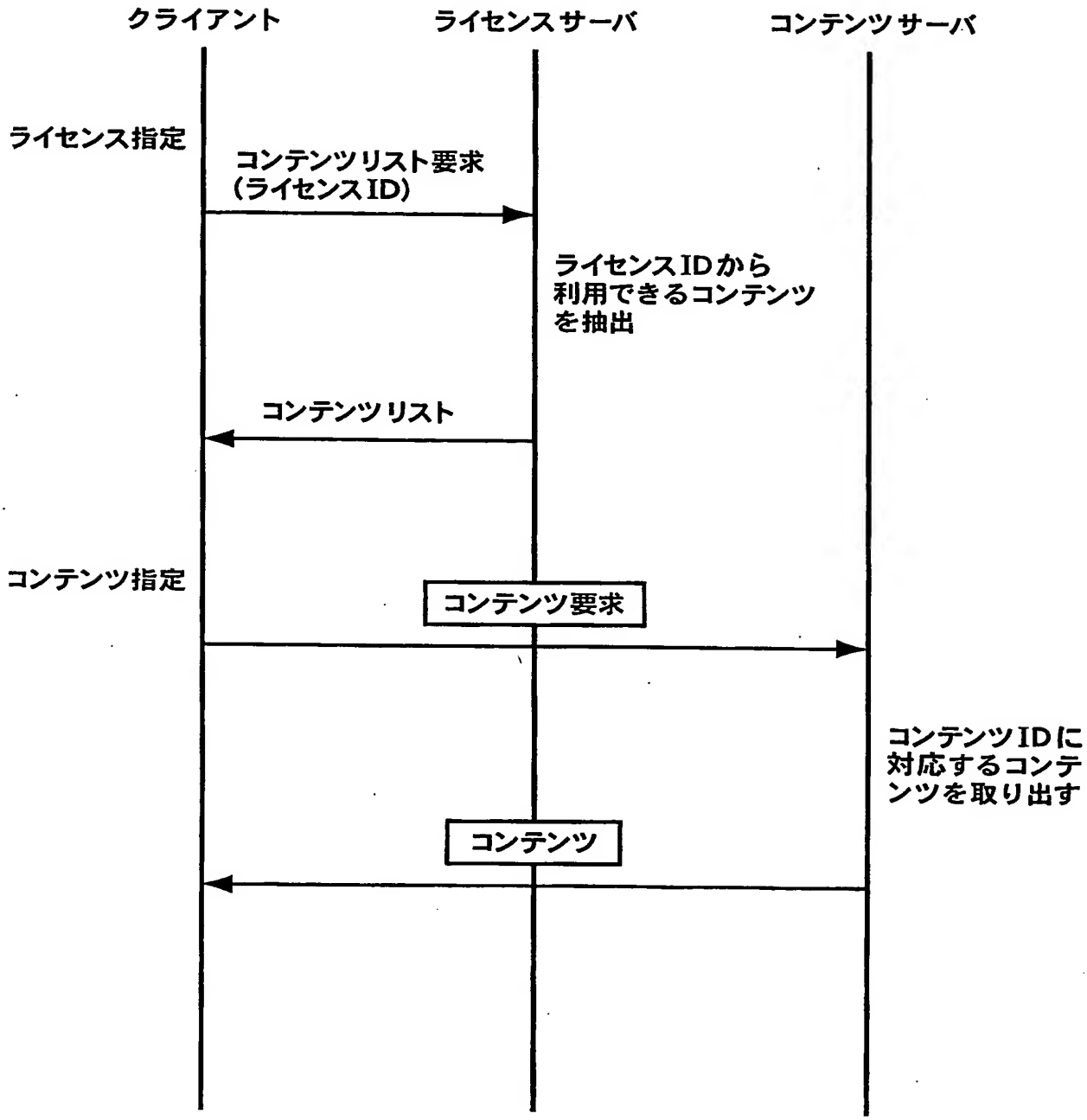

クライアント
ライセンスサーバ
コンテンツサーバ
ライセンス指定
コンテンツリスト要求
（ライセンスID）
ライセンスIDから
利用できるコンテンツ
を抽出
コンテンツリスト
コンテンツ指定
コンテンツ要求
コンテンツIDに
対応するコンテ
ンツを取り出す
コンテンツ

図14

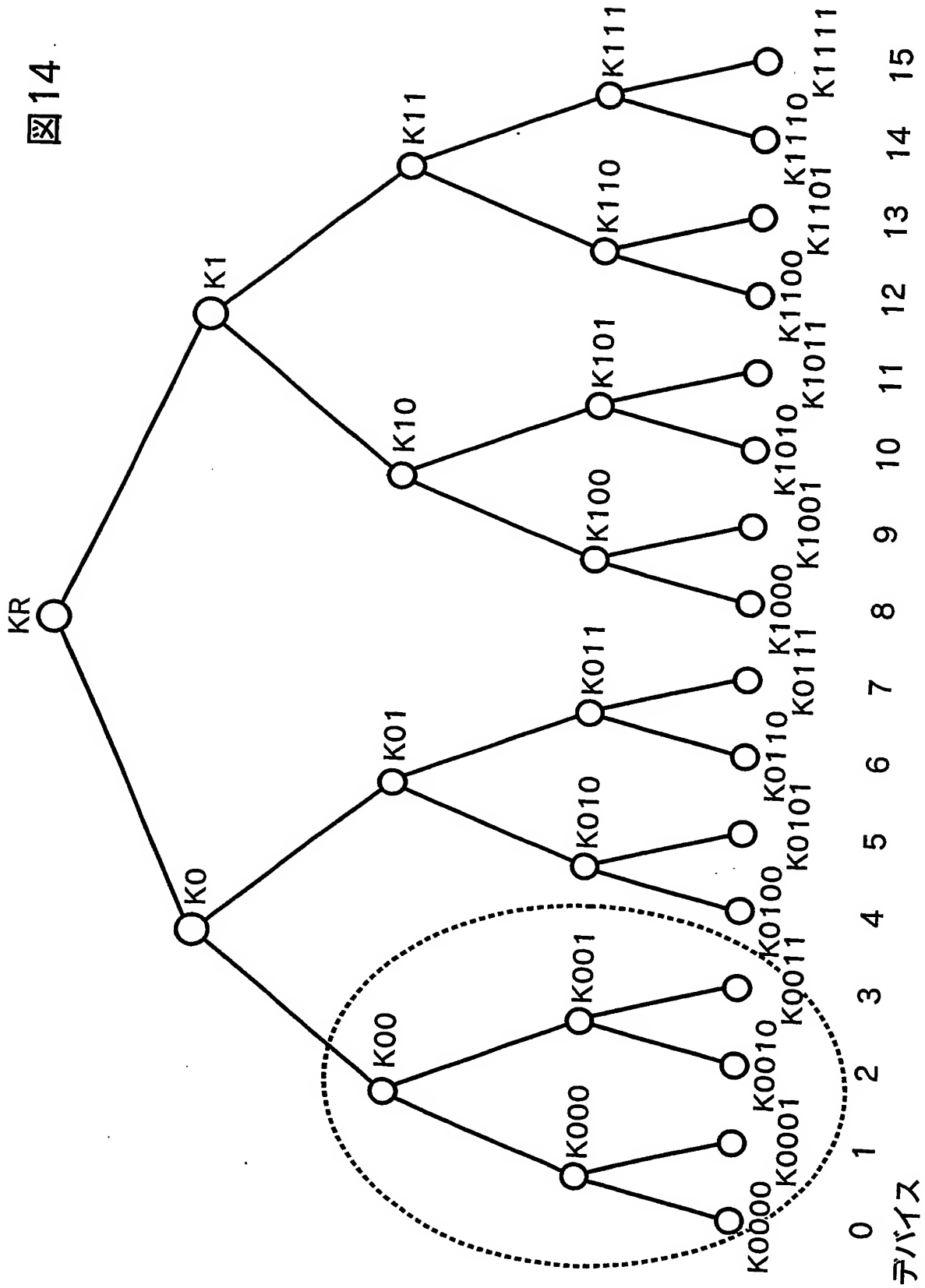

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

図15

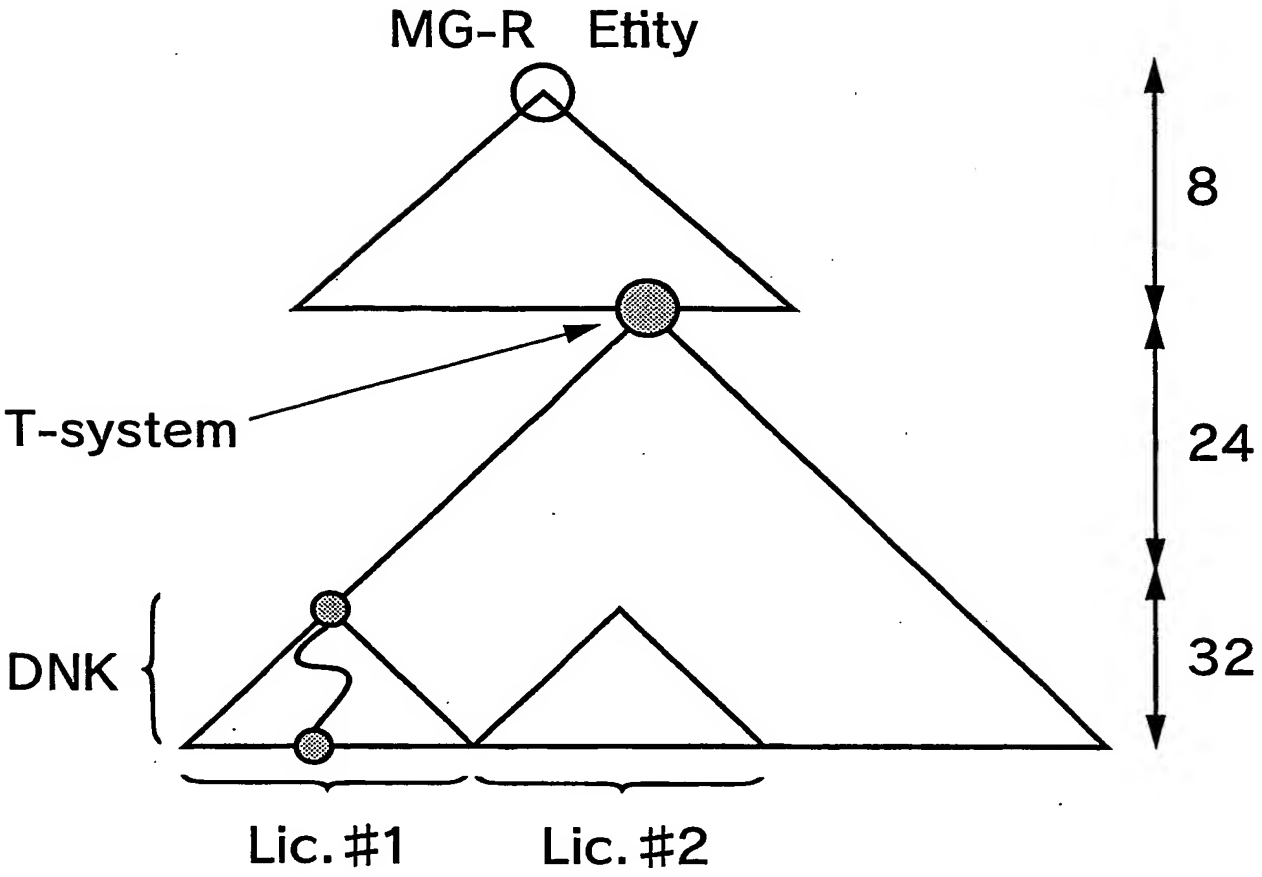
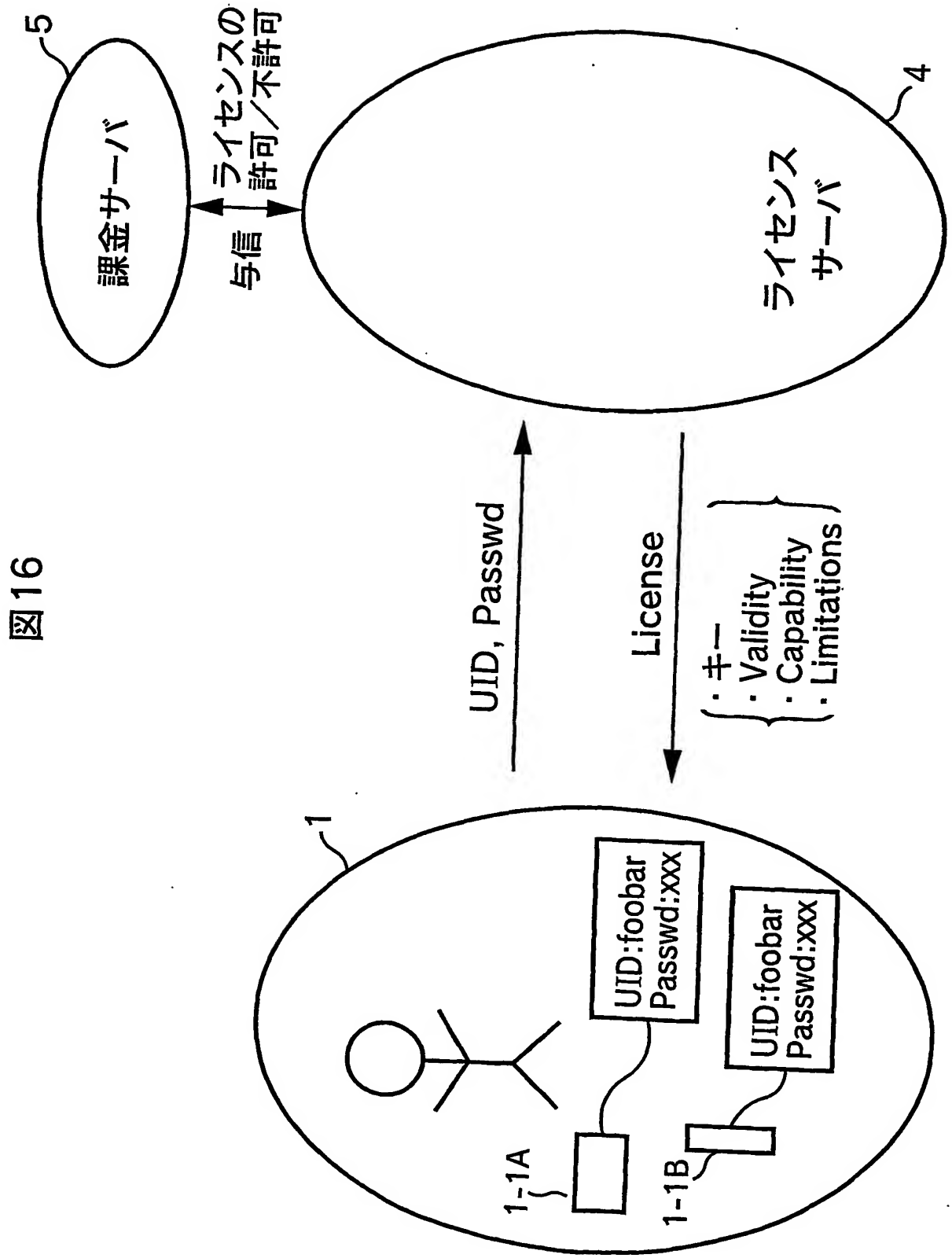


図16


5
課金サーバ
ライセンスの
許可／不許可
与信
4
ライセンス
サーバ
UID, Passwd
License
・キー
・Validity
・Capability
・Limitations
1
UID:foobar
Passwd:xxx
UID:foobar
Passwd:xxx
1-1A
1-1B

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/12356

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, G06F17/60, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, G06F17/60, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

| | | | |
|---|---|---|---|
| Jitsuyo Shinan Koho | 1922-1996 | Toroku Jitsuyo Shinan Koho | 1994-2003 |
| Kokai Jitsuyo Shinan Koho | 1971-2003 | Jitsuyo Shinan Toroku Koho | 1996-2003 |

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE(JOIS), WPI, INSPEC(DIALOG), content, attribute, metadata

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | JP 7-74744 A (Waseda University), 17 March, 1995 (17.03.95), Par. Nos. [0022], [0052] to [0053] (Family: none) | 1-5,9-11 |
| Y | JP 2000-293439 A (Fujitsu Ltd.), 20 October, 2000 (20.10.00), Par. Nos. [0069], [0107] to [0108] (Family: none) | 1-5,9-11 |
| Y | "Juraigata Mole o Kakucho shita Online Contents Hanbai System", Information Processing Society of Japan Kenkyu Hokoku, Vol.99, No.11, pages 87 to 93 (99-EIP-3), 30 January, 1999 (30.01.99), 4.3.1 Kenri Hogo Contents Kozo | 2 |

[x] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| | |
|---|---|
| Date of the actual completion of the international search<br>07 March, 2003 (07.03.03) | Date of mailing of the international search report<br>18 March, 2003 (18.03.03) |
| Name and mailing address of the ISA/<br>Japanese Patent Office<br><br>Facsimile No. | Authorized officer<br><br>Telephone No. |

Form PCT/ISA/210 (second sheet) (July 1998)

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/12356

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | JP 7-105231 A (Nippon Telegraph And Telephone Corp.),<br>21 April, 1995 (21.04.95),<br>Par. No. [0026]<br>(Family: none) | 1-5,9-11 |
| A | JP 2000-188744 A (Kabushiki kaisha Jisedai Joho Hoso System Kenkyusho),<br>04 July, 2000 (04.07.00),<br>Par. Nos. [0079] to [0085]<br>(Family: none) | 1-5,9-11 |
| A | EP 1107137 A2 (International Business Machines Corp.),<br>13 June, 2000 (13.06.00),<br>All pages<br>& JP 2001-274788 A & CN 1306259 A | 1-5,9-11 |
| A | US 2001/0042111 A1 (Matsushita Electric Industrial Co., Ltd.),<br>15 November, 2001 (15.11.01),<br>All pages<br>& EP 116084 A2 & JP 2001-318848 A<br>& CN 1326145 A | 1-5,9-11 |

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/12356

**Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims of the present application are divided into the following three groups:
1. Claims 1-5, 9-11
2. Claims 6,7
3. Claim 8

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: 1-5, 9-11

**Remark on Protest**

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号 PCT／JP02／12356

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ H04L9／08, G06F17／60, G06F15／00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ H04L9／08, G06F17／60, G06F15／00

最小限資料以外の資料で調査を行った分野に含まれるもの

| | |
|---|---|
| 日本国実用新案公報 | 1922－1996年 |
| 日本国公開実用新案公報 | 1971－2003年 |
| 日本国登録実用新案公報 | 1994－2003年 |
| 日本国実用新案登録公報 | 1996－2003年 |

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JICSTファイル（JOIS），WPI，INSPEC（DIALOG）
content, attribute, metadata

C. 関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| Y | JP 7-74744 A（学校法人早稲田大学）<br>1995.03.17, 第22, 52-53段落 （ファミリなし） | 1-5, 9-11 |
| Y | JP 2000-293439 A（富士通株式会社）<br>2000.10.20, 第69, 107-108段落 （ファミリなし） | 1-5, 9-11 |
| Y | 従来型電子モールを拡張したオンラインコンテンツ販売システム，情報処理学会研究報告，Vol.99 No.11, p.87-93（99-EIP-3）<br>1999.01.30, 4.3.1権利保護コンテンツ構造 | 2 |

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

| | |
|---|---|
| 国際調査を完了した日<br>07.03.03 | 国際調査報告の発送日<br>18.03.03 |
| 国際調査機関の名称及びあて先<br>日本国特許庁（ISA／JP）<br>郵便番号100－8915<br>東京都千代田区霞が関三丁目4番3号 | 特許庁審査官（権限のある職員）<br>中里 裕正 5M 9364<br>電話番号 03－3581－1101 内線 3597 |

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０２／１２３５６

C（続き）．　関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| A | JP 7-105231 A (日本電信電話株式会社)<br>1995.04.21, 第26段落　(ファミリなし) | 1-5, 9-11 |
| A | JP 2000-188744 A (株式会社次世代情報放送システム研究所)<br>2000.07.04, 第79-85段落　(ファミリなし) | 1-5, 9-11 |
| A | EP 1107137 A2 (International Business Machines Corporation)<br>2000.06.13, 全頁を参照 & JP 2001-274788 A & CN 1306259 A | 1-5, 9-11 |
| A | US 2001/0042111 A1(Matsushita Electric Industrial Co., Ltd.)<br>2001.11.15, 全頁を参照 &<br>EP 116084 A2 & JP 2001-318848 A & CN 1326145 A | 1-5, 9-11 |

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０２／１２３５６

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2. ☐ 請求の範囲 _____は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3. ☐ 請求の範囲 _____は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

本願の請求の範囲に係る発明は、以下の３群に分けられるものと認める。

1．請求の範囲 1-5, 9-11
2．請求の範囲 6, 7
3．請求の範囲 8

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4. ☒ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

請求の範囲 1-5, 9-11

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。